STATE OF ALABAMA

Information Technology Standard

Standard 640-02S2: Virtual Private Networks

1. INTRODUCTION:

A Virtual Private Network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. VPN is the preferred method for users to remotely access (from homes, hotels, off-site offices, etc.) State of Alabama information system resources.

2. OBJECTIVE:

Define requirements for secure remote access VPN connections into the State network.

3. SCOPE:

These requirements apply to all State of Alabama employees, contractors, vendors, and business partners authorized VPN access to the State network (Users), to all personnel responsible for the administration of VPN services and devices (Administrators), and to all Managers responsible for authorizing VPN usage.

4. REQUIREMENTS:

Based on the recommendations of the National Institute of Standards and Technology (NIST) as set forth in Special Publication 800-77: Guide to IPSec VPNs, State of Alabama organizations that deploy and/or manage virtual private networks shall comply with the following requirements:

4.1 VPN MANAGEMENT

Requests for VPN connectivity require the written approval of the agency IT Manager.

VPN connections with business partners and other non-State entities requires a written interconnection agreement defining the rules of behavior and security controls that must be maintained and the terms and conditions for sharing data and information resources.

Any VPN solution used for business partner connectivity shall be properly configured to limit or filter access to specific and necessary information resources. The connection shall allow monitoring.

VPN access accounts shall be reviewed at least quarterly. Inactive accounts shall be disabled in accordance with access management requirements.

VPN access may be terminated at any time for reasons including, but not limited to, termination of service provider agreements, changes in or termination of employment, request by the system/data owner, non-compliance with security policies, or negative impact on overall network performance attributable to VPN communications.

4.2 VPN ADMINISTRATION

4.2.1 Authentication

Enforce user authentication at the access point before granting VPN access to State network resources. VPN access and authentication shall comply with normal network access policies and procedures (including password standards, log-in attempts, lock-out policy, etc).

Users may authenticate using their domain login when a trust relationship can be established between the RADIUS server and the user's Domain Controller.

When a trust relationship cannot be established, create locally administered user accounts on either the RADIUS server or the VPN Concentrator.

4.2.2 Secure Host

Systems and networks at the VPN endpoints must meet all the security policies and standards applicable to other State systems and networks.

All hosts, including privately owned personal computers, connected to State networks via VPN must have up-to-date and properly configured anti-virus software and current operating system service pack and patch level. Hosts may be scanned to ensure compliance with State standards, and users may be denied VPN access if their host system presents an unacceptable risk to State networks.

4.2.3 Controls

VPN communications shall utilize encryption consistent with State encryption standards.

Terminate the VPN outside the firewall such that VPN traffic is visible to network IDS.

Split tunneling is not permitted. All traffic to and from the VPN client shall be routed through the VPN tunnel; all other traffic shall be dropped.

Users connected via VPN shall not be allowed simultaneous access to the Internet.

Monitor VPN usage on a regular basis for security and performance. Any unusual VPN event that may indicate unauthorized use of VPN services shall immediately be reported as a cyber security incident following applicable reporting procedures.

5. DEFINITIONS:

RADIUS: Remote Authentication Dial-In User Service, RADIUS, is an authentication, authorization, and accounting (AAA) protocol for network access application.

SPLIT TUNNELING: Term used to describe a multiple-branch networking path. In a VPN context, a secure tunnel is established to the VPN concentrator and other traffic is sent directly to different remote locations without passing through the VPN concentrator. This can expose the State's networked resources to attack and can make State resources accessible to anyone from non-trusted networks.

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 640-02: Remote Access

6.2 RELATED DOCUMENTS

Information Technology Standard 640-01S1: Interconnecting IT Systems

Information Technology Standard 620-01S1: Access Management

Signed by Eugene J. Akers, Ph.D., Assistant Director

Revision History

Version	Release Date	Comments
Original	2/16/2007	